Layer 2 SGT Imposition and Forwarding

Feature History for Layer 2 SGT Imposition and Forwarding

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	Layer 2 SGT Imposition and Forwarding: Layer 2 SGT Imposition and Forwarding enables interfaces on a switch to be manually configured for Cisco TrustSec, allowing the switch to insert a SGT into network packets	Cisco C9610 Series Smart Switches

Layer 2 SGT Imposition and Forwarding

Layer 2 SGT Imposition and Forwarding features enables interfaces on a switch to be manually configured for Cisco TrustSec, allowing the switch to insert a SGT into network packets. The SGT is carried throughout the network in the Cisco TrustSec header, enabling consistent security group policy enforcement across the infrastructure.

Guidelines to configure Layer 2 SGT Imposition and Forwarding

The Cisco Trustsec network needs to be established with the following prerequisites before implementing the Layer 2 SGT Imposition and Forwarding feature:

- Connectivity exists between all network devices
- Cisco Secure Access Control System (ACS) 5.1 operates with a Cisco TrustSec -SXP license
- Directory, DHCP, DNS, certificate authority, and NTP servers function within the network
- Configure the retry open timer command to a different value on different routers.

How to Configure SGT Handling: L2 SGT Imposition and Forwarding

These sections provide configuration information for SGT Handling: L2 SGT Imposition and Forwarding.

Enable Layer 2 SGT Imposition and Forwarding Manually on an Interface

Perform this task to manually enable an interface on the device for Cisco TrustSec so that the device can add SGT in the packet to be propagated throughout the network and to implement a static authorization policy.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** {**GigabitEthernet** *port* | **Vlan** *number*}

Example:

```
Device(config)# interface gigabitethernet 0
```

Enters the interface on which CTS SGT authorization and forwarding is enabled.

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

Enables the interface for CTS SGT authorization and forwarding, and enters CTS manual interface configuration mode.

Step 5 **policy static sgt** *tag* [**trusted**]

Example:

```
Device(config-if-cts-manual)# policy static sgt 100 trusted
```

Configures a static authorization policy for a CTS security group with a tagged packet that defines the trustworthiness of the SGT.

Step 6 **end**

Example:

```
Device(config-if-cts-manual)# end
```

Exits CTS manual interface configuration mode and enters privileged EXEC mode

Step 7 **show cts interface** [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

Example:

```
Device# show cts interface brief
```

Displays CTS configuration statistics for the interface.

Disable CTS SGT Propagation on an Interface

Follow these steps to disable CTS SGT Propagation on an interface in an instance when a peer device is not capable of receiving an SGT.

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** {**GigabitEthernet** *port* | **Vlan** *number*}

Example:

```
Device(config)# interface gigabitethernet 0
```

Enters the interface on which CTS SGT authorization and forwarding is enabled

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

Enables the interface for CTS SGT authorization and forwarding.

CTS manual interface configuration mode is entered where CTS parameters can be configured.

Step 5 **no propagate sgt**

Example:

```
Device(config-if-cts-manual)# no propagate sgt
```

Disables CTS SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT.

Note
CTS SGT propagation is enabled by default. The **propagate sgt** command can be used if CTS SGT propagation needs to be turned on again for a peer device.

Once the **no propagate sgt** command is entered, the SGT tag is not added in the L2 header.

Step 6 **end**

Example:

```
Device(config-if-cts-manual)# end
```

Exits CTS manual interface configuration mode and enters privileged EXEC mode.

Step 7 **show cts interface** [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

Example:

```
Device# show cts interface brief
```

Displays CTS configuration statistics to verify that CTS SGT propagation was disabled on interface.